Données à caractère personnel : cartographie des traitements et registre des activités de traitement, quelles différences ? L'un peut-il remplacer l'autre ?

Le RGPD dans son article 30 rend obligatoire le Registre des activités de traitement pour certaines entreprises. La Cartographie des Traitements, même si elle n'est pas exigée formellement par le RGPD, est quant à elle indispensable dans la pratique pour toutes les entreprises car elle est au coeur de la démarche de conformité au RGPD.

Quelles sont les caractéristiques principales de ces outils qui, pour des raisons diverses, apparaissent comme indispensables ? Bien qu'ils semblent proches, sont-ils pour autant équivalents ou interchangeables ?

Le Registre des activités de traitement, une obligation légale

Le Registre des activités de traitement est un outil obligatoire pour toutes les organisations de plus de 250 salariés. Les entreprises de moins de 250 salariés ne sont donc pas dans l'obligation de mettre en place un Registre des activités de traitements, sauf :

-pour un traitement susceptible de comporter un risque pour les droits et les libertés des personnes concernées, s'il n'est pas occasionnel, ou s'il porte notamment sur les catégories particulières de données (données sensibles – art 9 RGPD),
-sur des DCP relatives à des condamnations pénales.

Ainsi, si une entreprise de moins de 250 salariés a des traitements qui rentrent dans une de ces catégories, ils devront figurer dans un Registre des activités de traitement.
Si l'organisation est éligible à mise en place du Registre, mais qu'il n'a pas été instauré, elle s'expose à des sanctions de l'autorité de contrôle, la CNIL en France. Le montant de la sanction pourra s'élever jusqu'à 10 000 000 € ou dans le cas d'une entreprise jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Dans les organisations éligibles, le Registre des activités de traitement permet de recenser formellement les traitements de données à caractère personnel en présentant de manière synthétique l'objet du traitement, sa base légale, les données collectées, les durées de conservation, les mesures de protections organisationnelles et techniques en place, les personnes concernées, les destinataires de données, les sous-traitants, la présence de transferts hors UE.

Toutefois, le Registre des activités de traitement, tel que requis par l'article 30 du RGPD, n'est pas suffisant pour atteindre et maintenir la conformité. Tout d'abord, les informations demandées ne couvrent pas toutes les exigences requises par le RGPD pour que le traitement soit considéré

comme conforme. Ensuite, en cas de non-conformité ou d'évolutions des caractéristiques des traitements, il ne permet pas de suivre les actions nécessaires. C'est face à ces deux limites que la cartographie des traitements devient indispensable.

La cartographie des traitements, un passage obligé pour le pilotage de la conformité

Cet outil (privilégier Excel), est un support au diagnostic et à l'analyse des écarts de conformité. Il permet d'identifier le plan d'action à court, moyen et long terme pour la conformité. Pour ce faire, il faut, via la cartographie des traitements, décortiquer chaque traitement sous tous ses angles en abordant tous les éléments de conformité décrits à l'instant T.

Dans un premier temps, il faudra décrire les éléments inhérents au traitement : nom du traitement, détail du processus, personnes concernées, données collectées, catégories des données, volume de données concernées, finalités, pertinence, destinataires, durées de conservation en base active et en archive, modalités de conservation, obligations légales (consentement, intérêt légitime, obligation légale, contrat), droit d'information, droit d'opposition/accès/rectification/portabilité, formalités, modalités de collecte directe/ indirecte, mesures pour assurer l'intégrité des données, modalités d'échanges des données, application(s) utilisée(s).

Dans un deuxième temps, il faudra décrire les éléments inhérents aux applications utilisées pour le traitement : traitement(s) concerné(s), nom de l'application, prestataire, description, gestion des accès, durées de conservation, modalités de suppression des données, mesures de sécurité (disponibilité, intégrité, confidentialité, traçabilité), flux entre applications, hébergement.
Grâce à la collecte de ces informations et à l'analyse des écarts, la cartographie permettra :

-d'alimenter le Registre des activités de traitement,
-de mettre en place un plan d'action pour la conformité,
-de suivre la conformité dans le temps.

Une complémentarité nécessaire des deux outils

Aussi, que vous ayez déjà entamé votre démarche de conformité ou que vous deviez commencer, il est indispensable d'effectuer une cartographie des traitements en complément de la mise en place du Registre des activités de traitement.

La cartographie peut être la pierre angulaire de toute votre démarche de conformité avec le RGPD. Elle fournira les éléments indispensables pour initier le Registre des traitements et pour l'alimenter ; elle permettra de dégager les points clés du plan de mise en conformité et, dans la durée, elle permettra, à travers ses mises à jour régulières, de suivre l'implémentation du plan de mise en conformité. Cet outil sera la preuve de votre maitrise de la conformité de vos traitements.

Francesca SERIO – Consultant Senior chez Provadys / NetXP